

Introduction to Internet Explorer 7

Microsoft has released Internet Explorer 7 (IE 7). Because of certain security features, it is imperative that Internet Options be modified before logging into any Infinite Campus application.

Infinite Campus, Inc. is publishing this document because Microsoft is promoting the update to IE7 as a mandatory critical update using the Windows Update mechanism. Technical administrators at school districts may use this mechanism to keep their machines patched with the latest security vulnerabilities automatically.

The Infinite Campus application has been tested against IE7 and it was found that there were considerable performance issues with phishing filters being set to the “on” or “off” selections instead of being “disabled.”

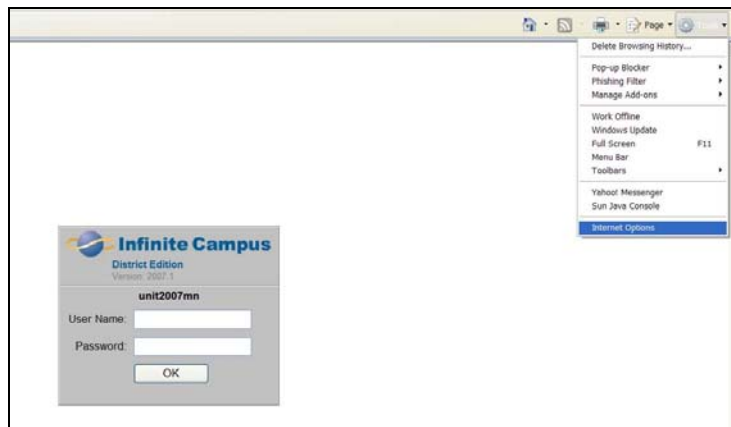
Phishing is one of the fastest growing threats on the Internet and a form of identity theft. It refers to high-tech scams using phony Web sites with actual brands designed to steal valuable personal information such as user names, passwords, credit card numbers and Social Security numbers.

Described below are two ways to eliminate the performance issues that users may experience.

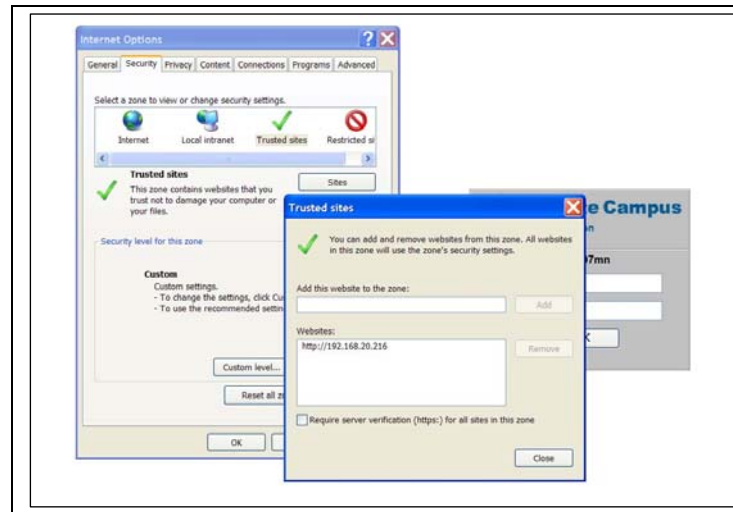
Adding the Infinite Campus site to the list of trusted sights

Adding sites to the trusted site zones turns off phishing filters on only those selected sites.

1. Download Internet Explorer 7.
2. After restarting the computer, launch the browser. A pop-up window may appear asking the user to set up phishing filters. Choose the recommended option of **Turn on Automatic Phishing Filter**. Click **OK**.
3. Go to the login page of an Infinite Campus site. **DO NOT LOG IN**.
4. Select the **Tools** option on the right hand side of the screen in the toolbar.



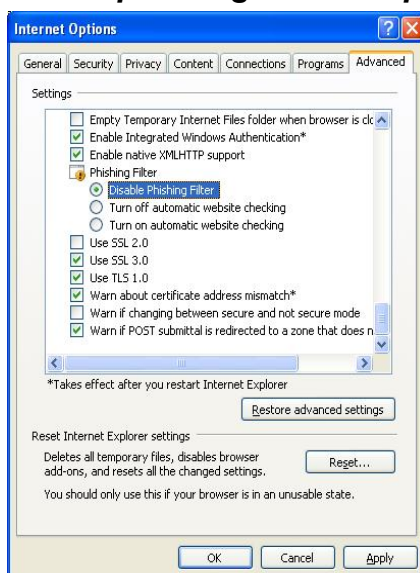
5. Select **Internet Options**.
6. Select the **Security** tab and then select the **Trusted Sites** option.



7. Click the **Sites** button. The Infinite Campus login address will be listed in the *Add this website to the zone* field.
8. Uncheck the *Require server verification (https:)* checkbox.
9. Click the **Add** button.
10. Check the server verification checkbox again.
11. Click the **Close** button.

In order for this change to take affect, the browser window may need to be closed and reopened.

Disable the phishing filter completely for ALL sites:



1. Select the **Tools** option on the right hand side of the screen in the tool bar.
2. Select **Internet Options**.
3. Go to the **Advanced** tab.
4. Scroll to the **Security** setting and locate the **Phishing Filter**.
5. Select the **Disable Phishing Filter** option.
6. Click the **OK** button. Restart the browser.